ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 109 (2004) 41–58

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

The density of elliptic curves having a global minimal Weierstrass equation

Ebru Bekyel*

Sabancı University, FENS, Tuzla 34956, Istanbul, Turkey

Received 12 November 2002; revised 5 January 2004

Communicated by G. Wüstholz

Available online 3 September 2004

Abstract

We show that a positive density of elliptic curves over a number field counted using their short Weierstrass equations belong to a given Weierstrass class and in particular, a positive density of elliptic curves have a global minimal Weierstrass equation. The density is given by a ratio of partial zeta functions of the number field K evaluated at 10 with some extra factors for the bad primes.

Keywords: Elliptic curve; Weierstrass equation; Zeta function

1. Introduction

Let K be a number field, E an elliptic curve over K given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

with discriminant Δ and $a_1, a_2, a_3, a_4, a_6 \in O_K$. Such an equation is a *global minimal Weierstrass equation* for E/K if the discriminant has minimal valuation at each non-Archimedean prime. In this paper, we study what fraction of elliptic curves over K have a global minimal equation. For each non-Archimedean valuation $v \in M_K^0$, let K_v

* Fax: 90-216-483-9550.
E-mail address: ebekyel@sabanciuniv.edu (E. Bekyel).

0022-314X/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2004.06.003

be the local field which is the completion of K at v. For each such v we can find a Weierstrass equation for E over K_v

$$y_v^2 + a_{1,v}x_v y_v + a_{3,v}y_v = x_v^3 + a_{2,v}x_v^2 + a_{4,v}x_v + a_{6,v} \tag{2}$$

with $a_{1,v}, a_{3,v}, a_{2,v}, a_{4,v}, a_{6,v} \in O_v$ such that the discriminant Δ_v has minimal valuation. The minimal discriminant of E/K is defined to be the integral ideal

$$\mathfrak{D}_{E/K} = \prod_{v \in M_K^0} \mathfrak{p}_v^{v(\Delta_v)},$$

where $\mathfrak{p}_v$ is the prime ideal associated to v. Thus, a global minimal Weierstrass equation for E/K is one where $(\Delta) = \mathfrak{D}_{E/K}$. Let

$$x = u_v^2 x_v + r_v, \qquad y = u_v^3 y_v + s_v u_v^2 x_v + t_v$$

be the change of coordinates producing Eq. (2) from Eq. (1). The Weierstrass class of E/K is the class of the ideal

$$\mathfrak{a}_\Delta = \prod_{v \in M_K^0} \mathfrak{p}_v^{-v(u_v)}$$

in the class group H_K of K. It is well known [6, p. 225] that E/K has a global minimal Weierstrass equation if and only if the Weierstrass class of E/K is trivial. In particular, if K has class number 1 then E will always have a global minimal Weierstrass equation. In general, Silverman [5] has shown that for every $\mathfrak{C}$ in the ideal class group of K there exists an elliptic curve E/K whose Weierstrass class equals $\mathfrak{C}$. This problem is similar to the existance of a relative integral basis for a quadratic extension of a number field K. Fröhlich [2] has shown that this problem is also equivalent to the triviality of a certain ideal class in K. In this paper we will look at the density of elliptic curves over a number field whose Weierstrass class equals a particular $\mathfrak{C}$.

Theorem 1. *Let K be a number field and let $\mathfrak{C}$ be an ideal class in the ideal class group of K. For $A, B \in O_K$, let*

$$H([A, B, 1]) = \prod_v \max\{|A|_v, |B|_v, 1\}$$

be the usual height on projective space. Let $N(\mathfrak{C}, t)$ be the number of $A, B \in O_K$ such that $y^2 = x^3 + Ax + B$ defines an elliptic curve with $\mathfrak{a}_\Delta$ in $\mathfrak{C}$ and $H([A, B, 1]) \leqslant t$

and let $D(t) = \sum_{\mathfrak{C}} N(\mathfrak{C}, t)$. *Then the asymptotic density of elliptic curves having Weierstrass class equal to* $\mathfrak{C}$ *is given by*

$$\lim_{t\to\infty} \frac{N(\mathfrak{C}, t)}{D(t)} = \frac{1}{h_K \zeta_K(10)} \sum_{\mathfrak{D}} \zeta_K(\mathfrak{D}, 10) f_K(\mathfrak{C}\mathfrak{D}),$$

where $\zeta_K(s)$ *is the Dedekind zeta function,* $\zeta_K(\mathfrak{D}, s)$ *is the partial zeta function for an ideal class* $\mathfrak{D}$ *of K, the sum is over all ideal classes and the constants* $f_K(\mathfrak{D})$ *are real numbers defined in Proposition* 10 *which can be calculated using at most the finitely many primes of K dividing* 6. *Moreover, this density is a positive number for any class* $\mathfrak{C}$.

There are many cases in which $f_K(\mathfrak{D}_0) = h_K$ for the trivial class $\mathfrak{D}_0$ and zero otherwise. For example, this true if every prime above 2 is principal and every ramified prime above 3 is principal, in which case we have a much simpler formula for the density given by

$$\frac{\zeta_K(\mathfrak{C}^{-1}, 10)}{\zeta_K(10)},$$

where $\zeta_K(\mathfrak{C}, s)$ is the partial zeta function summing over ideals in $\mathfrak{C}$ only.

We begin by finding local conditions for the values $v(u_v)$. Then we will count equations which have $\mathfrak{a}_\Delta$ equal to a fixed $\mathfrak{m}$ and then we will sum over all $\mathfrak{m}$ in the given ideal class and calculate the density. Finally we will do an example.

2. Local characterization

Let K be a local field with valuation v, valuation ring O and maximal ideal $\mathfrak{p}$. We will assume that the characteristic of K is not equal to 2 or 3. Let $A, B \in O$ define an elliptic curve

$$E : y^2 = x^3 + Ax + B \tag{3}$$

over K. Let

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4}$$

be a minimal equation for E and

$$x = u^2x + r, \qquad y = u^3y + sux^2 + t \tag{5}$$

with $u, r, s, t \in O$ be the change of variables from (3) to (4). Then $v(u)$ depends only on A and B and is independent of the particular minimal equation [6, Chapter VII, Proposition 1.3(b)]. Let f to be the function that assigns the non-negative integer $v(u)$ to a pair $A, B \in O$ as described above. For an integer $b \geqslant 1$ and any integer $k \geqslant 0$, let C_k be the image of $f^{-1}(k)$ under the natural surjection $O \times O \to O/\mathfrak{p}^{6(k+b)} \times O/\mathfrak{p}^{6(k+b)}$. Then by definition

$$f(A, B) = k \Rightarrow \left(\bar{A}, \bar{B}\right) \in C_k$$

and if b is chosen carefully, the converse will also hold as the next proposition shows.

Proposition 2. *Let K be a local field with valuation v, valuation ring O and maximal ideal $\mathfrak{p}$. There exists an integer $b \geqslant 1$ depending on the field K such that*

$$f(A, B) = k \Leftrightarrow \left(\bar{A}, \bar{B}\right) \in C_k,$$

where the sets C_k are defined above. We can always take $b = 1 + 5v(2) + 2v(3)$ although sometimes a smaller value will suffice.

Proof. Let $b = 1 + 5v(2) + 2v(3)$. For any $k \geqslant 0$, we need to show that $f(A, B) = k$, $A \equiv A' \bmod \mathfrak{p}^{6(b+k)}$ and $B \equiv B' \bmod \mathfrak{p}^{6(b+k)}$ implies $f\left(A', B'\right) = k$. So assume $f(A, B) = k$. This means there exists a change of variables as in Eq. (5) with $v(u) = k$. With this change of variables the a_1,..,a_6 in Eq. (4) are given by

$$a_1 = \frac{2s}{u}, \qquad a_2 = \frac{3r - s^2}{u^2}, \qquad a_3 = \frac{2t}{u^3},$$

$$a_4 = \frac{A + 3r^2 - 2st}{u^4}, \qquad a_6 = \frac{B + Ar + r^3 - t^2}{u^6}.$$

Since $A \equiv A' \bmod \mathfrak{p}^{6(b+k)}$ there exists $\alpha \in \mathfrak{p}^{6(b+k)}$such that $A' = A + \alpha$ and similarly there exists $\beta \in \mathfrak{p}^{6(k+b)}$ such that $B' = B + \beta$. Then the same change of variables applied to

$$y^2 = x^3 + A'x + B' \tag{6}$$

gives

$$y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6' \tag{7}$$

with

$$a_1' = a_1, \quad a_2' = a_2, \quad a_3' = a_3, \quad a_4' = a_4 + \frac{\alpha}{u^4}, \quad a_6' = a_6 + \frac{\beta + \alpha r}{u^6}.$$

Now, $a_1', a_2', a_3' \in O$ since a_1, a_2, a_3 are. For the last two

$$v\left(a_4'\right) \geqslant \min\left\{v\left(a_4\right), v\left(\alpha\right) - 4v\left(u\right)\right\} \geqslant 0$$

since $v\left(\alpha\right) - 4v\left(u\right) \geqslant 6\left(k+b\right) - 4k \geqslant 0$ and

$$v\left(a_6'\right) \geqslant \min\left\{v\left(a_6\right), v\left(\beta + \alpha r\right) - 6v\left(u\right)\right\} \geqslant 0$$

since $v\left(\beta + \alpha r\right) - 6v\left(u\right) \geqslant 6\left(k+b\right) - 6k \geqslant 0$. All of this implies that the new equation has coefficients in O and hence $f\left(A', B'\right) \geqslant k$. If $f\left(A', B'\right) > k$, then there would exist a change of variables this time for Eq. (6) with $v\left(u\right) = k+1$ resulting in an equation with coefficients a_i' in O. Then we claim that the same change of variables applied to Eq. (3) would have integer coefficients. Similar to the above situation the only ones we need to check are a_4 and a_6 because the others are the same in both equations. Using the fact that $b \geqslant 1$ we have

$$v\left(a_4\right) = v\left(a_4' - \frac{\alpha}{u^4}\right) \geqslant \min\left\{v\left(a_4'\right), v\left(\alpha\right) - 4v\left(u\right)\right\} \geqslant 0$$

since $v\left(\alpha\right) - 4v\left(u\right) \geqslant 6\left(k+b\right) - 4\left(k+1\right) = 2k + 6b - 4 \geqslant 0$ and

$$v\left(a_6\right) = v\left(a_6' - \frac{\beta + \alpha r}{u^6}\right) \geqslant \min\left\{v\left(a_6'\right), v\left(\beta + \alpha r\right) - 6v\left(u\right)\right\} \geqslant 0$$

since $v\left(\beta + \alpha r\right) - 6v\left(u\right) \geqslant 6\left(k+b\right) - 6\left(k+1\right) = 6\left(b-1\right) \geqslant 0$ contradicting $f\left(A, B\right) = k$. Therefore $f\left(A', B'\right) = k$ and we are done. □

Remark 3. From now on when we write $\left(\bar{A}, \bar{B}\right) \in C_k$, it is understood that b is the integer in Proposition 2.

Proposition 4. *Let K be a local field and b and the C_k be defined as above. Let c_k be the number of elements in C_k. Then, for $k \geqslant b-1$ we have*

$$c_k = c_{b-1} N\mathfrak{p}^{2(k-b+1)}.$$

Proof. Fix a uniformizer π. For each $k \geqslant b-1$ define the map

$$\phi^k : C_k \to C_{b-1}$$
$$\left(A, B\right) \to \left(A\pi^{4(b-1-k)}, B\pi^{6(b-1-k)}\right).$$

First of all, this map can be defined because $f\left(A, B\right) = k$ implies that the Weierstrass equation $y^2 = x^3 + Ax + B$ has $v\left(c_4\right) \geqslant 4k$ and $v\left(c_6\right) \geqslant 6k$. Since $c_4 = -48A$ and $c_6 = -32 \cdot 9B$ we have $4v\left(2\right) + v\left(3\right) + v\left(A\right) \geqslant 4k$ and $5v\left(2\right) + 2v\left(3\right) + v\left(B\right) \geqslant 6k$. By choice of

b we have $v(A)+4(b-1-k) \geqslant 3(b-1) \geqslant 0$ and $v(B)+6(b-1-k) \geqslant 5(b-1) \geqslant 0$. The map is well-defined since

$$\begin{aligned} A \equiv A' \bmod \mathfrak{p}^{6(k+b)} &\Rightarrow A\pi^{4(b-1-k)} \equiv A'\pi^{4(b-1-k)} \bmod \mathfrak{p}^{2k+10b-4} \\ &\Rightarrow A\pi^{4(b-1-k)} \equiv A'\pi^{4(b-1-k)} \bmod \mathfrak{p}^{6(2b-1)} \end{aligned}$$

and

$$B \equiv B' \bmod \mathfrak{p}^{6(k+b)} \Rightarrow B\pi^{6(b-1-k)} \equiv B'\pi^{6(b-1-k)} \bmod \mathfrak{p}^{6(2b-1)}.$$

It is also onto because for $(A, B) \in C_{b-1}$ we have

$$(A, B) = \phi^k\left(A\pi^{4(k-b+1)}, B\pi^{6(k-b+1)}\right).$$

Finally, ϕ^k is $N\mathfrak{p}^{2(k-b+1)}$ to 1 because

$$\begin{aligned} A\pi^{4(b-1-k)} &\equiv A'\pi^{4(b-1-k)} \bmod \mathfrak{p}^{6(2b-1)} \Rightarrow A \equiv A' \bmod \mathfrak{p}^{8b+4k-2}, \\ B\pi^{6(b-1-k)} &\equiv B'\pi^{6(b-1-k)} \bmod \mathfrak{p}^{6(2b-1)} \Rightarrow B \equiv B' \bmod \mathfrak{p}^{6(k+b)} \end{aligned}$$

and $6(k+b) - (8b+4k-2) = 2(k-b+1)$ finishing the proof. □

Remark 5. If $b = 1$ the situation is very simple since for all $k \geqslant 0$ we have $c_k = c_0 \cdot N\mathfrak{p}^{2k}$. If $\mathrm{Char}(O/\mathfrak{p}) \neq 2, 3$ then $b = 1$ since $y^2 = x^3 + Ax + B$ is minimal if and only if $v(A) < 4$ or $v(B) < 6$. In this case

$$\begin{aligned} c_0 &= \#\left(\frac{\{(A, B) \in O \times O : v(A) < 4 \text{ or } v(B) < 6\}}{\mathfrak{p}^6 \times \mathfrak{p}^6}\right) \\ &= N\mathfrak{p}^{12} - \#\left(\frac{\{(A, B) \in O \times O : v(A) \geqslant 4 \text{ and } v(B) \geqslant 6\}}{\mathfrak{p}^6 \times \mathfrak{p}^6}\right) \\ &= N\mathfrak{p}^{12} - \#\left(\frac{\mathfrak{p}^4}{\mathfrak{p}^6} \times \frac{\mathfrak{p}^6}{\mathfrak{p}^6}\right) \\ &= N\mathfrak{p}^{12} - N\mathfrak{p}^2 \\ &= N\mathfrak{p}^{12}\left(1 - N\mathfrak{p}^{-10}\right). \end{aligned}$$

3. Counting

In this section we want to count the elliptic curves over a fixed number field K which have a global minimal Weierstrass equation. Let K be a number field with

ring of integers O_K. Since any elliptic curve over a number field can be given by a Weierstrass equation of the form

$$y^2 = x^3 + Ax + B$$

with $A, B \in O_K$ we will do this by counting the pairs (A, B). Therefore, we need a way to count pairs of integers. The most natural method is the use of the height function $H([A, B, 1])$. Also, the argument in the previous section shows that we will have to do counting modulo some congruences. Although we only need to count pairs, we will be more general and count d-tuples, the result of which is Proposition 7. Then we will use this with $d = 2$. The following lemma will be used in estimating the error term in the counting function.

Lemma 6. *Let K be a number field of degree $n = r_1 + 2r_2$ and let $\mathfrak{a}$ be an integral ideal. Let j be the canonical embedding of K into its Minkowski space $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Then $j(\mathfrak{a})$ has a basis whose fundamental domain F has the property that*

$$\text{diameter}(F) = \sup_{x,y \in F} |x - y| \leqslant C_K N\mathfrak{a}^{1/n},$$

where C_K is a constant depending only on n and the discriminant d_K of K.

Proof. Let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be a basis constructed by choosing $\mathbf{v}_1 \neq 0$ such that $|\mathbf{v}_1|$ is minimal and given $\mathbf{v}_1, \ldots, \mathbf{v}_i$ choose $\mathbf{v}_{i+1}$ with minimal length such that the set $\mathbf{v}_1, \ldots, \mathbf{v}_{i+1}$ is linearly independent. Then

$$\sup_{x,y \in F} |x - y| \leqslant \sum_{i=1}^{n} |\mathbf{v}_i| \leqslant n |\mathbf{v}_n|.$$

Let σ_i, $(\tau_i, \bar{\tau}_j)$ be the real and pairs of complex embeddings of K. For any non-zero vector $\mathbf{v}$ we have

$$\begin{aligned} \left|\mathbf{v}^2\right| = |j(a)|^2 &= \sum_{i=1}^{r_1} \sigma_i(a)^2 + \sum_{j=1}^{r_2} \left|\tau_j(a)\right|^2 \\ &\geqslant \frac{1}{2} \sum_{\sigma} |\sigma(a)|^2, \end{aligned}$$

where in the last sum σ runs through all embeddings of K into $\mathbb{C}$. Using the fact that the arithmetic mean is greater than or equal to the geometric mean we get that

$$|\mathbf{v}| \geqslant \sqrt{n/2} N\mathfrak{a}^{1/n}.$$

Using

$$|\mathbf{v}_1| \cdots |\mathbf{v}_n| \leqslant C\sqrt{|d_K|}N\mathfrak{a}$$

[1, p. 205] where C is a constant depending only on n we have

$$|\mathbf{v}_n| \leqslant \frac{C\sqrt{|d_K|}N\mathfrak{a}}{|\mathbf{v}_1| \cdots |\mathbf{v}_{n-1}|} \leqslant \frac{C\sqrt{|d_K|}N\mathfrak{a}^{1/n}}{(n/2)^{(n-1)/2}}.$$

We have the result with $C_K = \frac{C_n\sqrt{|d_K|}}{(n/2)^{(n-1)/2}}$. □

Proposition 7. *Let K be a number field of degree $n = r_1 + 2r_2$. Let $r = r_1 + r_2 - 1$ be the rank of its unit group. Given an integer $d \geqslant 1$, integral ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_d$ of K and $a_1, \ldots, a_d \in O_K$ let*

$$H([A_1, \ldots, A_d, 1]) = \prod_{v \in M_K} \max\{|A_1|_v, \ldots, |A_d|_v, 1\}$$

be the usual height on projective space and let $F(\mathfrak{a}_1, \ldots, \mathfrak{a}_d, t)$ be the number of elements in

$$\left\{(A_1, \ldots, A_d) \in O_K^d : A_i \equiv a_i \bmod \mathfrak{a}_i \text{ for } 1 \leqslant i \leqslant d, H([A_1, \ldots, A_d, 1]) \leqslant t\right\}.$$

Then,

$$F(\mathfrak{a}_1, \ldots, \mathfrak{a}_d; t) = \frac{C_{K,d}\,\mathrm{Vol}\,R(t)}{N\mathfrak{a}_1 \ldots N\mathfrak{a}_d} + \mathrm{O}\left(\frac{\mathrm{Vol}\,\partial R(t)}{N\mathfrak{a}_1 \ldots N\mathfrak{a}_d} \sum_{i=1}^{d} N\mathfrak{a}_i^{1/n}\right),$$

where $R(t)$ is the region in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ given by

$$R(t) = \prod_{i=1}^{r_1} \max\{|\mathbf{x}_{i1}|, \ldots, |\mathbf{x}_{id}|, 1\} \prod_{j=1}^{r_2} \max\left\{\mathbf{u}_{j1}^2 + \mathbf{v}_{j1}^2, \ldots, \mathbf{u}_{jd}^2 + \mathbf{v}_{jd}^2, 1\right\} \leqslant t$$

and $\partial R(t)$ is its boundary and the constants depend only on the field K and d.

Proof. Each $\mathfrak{a}_i$ is a complete lattice Λ_i in $\mathbb{R}^n$. Then $\Lambda = \oplus\Lambda_i$ is a complete lattice in $\mathbb{R}^{nd}$. The d-tuples $(A_1, \ldots, A_d)$ we want to count make up the translate of the lattice Λ by $(a_1, \ldots, a_d)$. So we want to count the number of lattice points l such that $l \in R_a(t)$

where $R_a(t)$ is the region $R(t)$ shifted by the image of $a = (a_1, \ldots, a_d)$. Following Lang [3, p. 225], the number of lattice points in $R(t)$ is given by $\operatorname{Vol} R(t) / \operatorname{Vol} F$ where F is a fundamental domain for the lattice Λ with an error term counting the number of lattice points l such that the translate of $F + l$ intersects the boundary $\partial R(t)$. Each Λ_i has volume of a fundamental domain given by $\sqrt{|d_K|} N\mathfrak{a}_i$ hence the volume of a fundamental domain for Λ is $|d_K|^{d/2} N\mathfrak{a}_1 \cdots N\mathfrak{a}_d$ which gives us the main term with $C_{K,d} = |d_K|^{-d/2}$. For the error term, if $F + l$ intersects the boundary for some $l \in \Lambda$ then $F + l$ is in the set

$$\mathbf{T}\left(\delta, \partial R(t)\right) = \left\{x \in \mathbb{R}^{nd} : \text{distance from } x \text{ to } \partial R(t) \leqslant \delta\right\}$$

with $\delta = \text{diameter}(F)$. The number of such l is less than or equal to the volume of $\mathbf{T}\left(\delta, \partial R(t)\right)$ divided by the volume of F. Since $\text{diameter}(F) \leqslant \sum_i \text{diameter}\left(F_{\mathfrak{a}_i}\right)$, $\operatorname{Vol}\left(\mathbf{T}\left(\delta, \partial R(t)\right)\right) = \mathrm{O}\left(\delta \operatorname{Vol} \partial R(t)\right)$ and the argument is still valid if we shift the region $R(t)$ using Lemma 6 we have the result. □

Remark 8. It is tedious but easy to show that the volume of the region $R(t)$ is given by

$$Ct^d (\log t)^r + \mathrm{O}\left(t^d (\log t)^{r-1}\right)$$

and the volume of its boundary is

$$Dt^d (\log t)^{r-1} + \mathrm{O}\left(t^d (\log t)^{r-2}\right),$$

where C and D are constants depending on d, r_1, r_2.

In the next proposition we will have to look at (A, B) modulo different prime powers. To show the dependence on the prime we will replace C_k, c_k, b defined in Section 2 with $C_k^{\mathfrak{p}}, c_k^{\mathfrak{p}}, b_{\mathfrak{p}}$.

Proposition 9. *Let K be a number field of degree n, $R(t)$ be the region defined in Proposition 7 and $\partial R(t)$ its boundary. For an ideal $\mathfrak{m} \subset O_K$, let $m_{\mathfrak{p}} = v_{\mathfrak{p}}(\mathfrak{m})$ and let*

$$G(\mathfrak{m}, t) = \#\left\{(A, B) : \left(\bar{A}, \bar{B}\right) \in C_{m_{\mathfrak{p}}}^{\mathfrak{p}} \text{ for all } \mathfrak{p}, H([A, B, 1]) \leqslant t\right\}.$$

Then

$$G(\mathfrak{m}, t) = C_K \alpha(K) f(\mathfrak{m}) \operatorname{Vol} R(t) + \mathrm{O}\left(g(\mathfrak{m}) \operatorname{Vol} \partial R(t)\right),$$

where C_K is the constant $C_{K,2}$ from Proposition 7,

$$\alpha(K) = \zeta_K(10)^{-1} \prod_{b_\mathfrak{p}>1} \frac{c_0^\mathfrak{p}}{\left(1 - N\mathfrak{p}^{-10}\right) N\mathfrak{p}^{12b_\mathfrak{p}}},$$

$$f(\mathfrak{m}) = \frac{1}{N\mathfrak{m}^{12}} \prod_{\mathfrak{p}|\mathfrak{m}} \frac{c_{m_\mathfrak{p}}^\mathfrak{p}}{c_0^\mathfrak{p}}$$

and

$$g(\mathfrak{m}) = \prod_{\mathfrak{p}|\mathfrak{m}} \left(\frac{c_{m_\mathfrak{p}}^\mathfrak{p}}{N\mathfrak{p}^{6(b_\mathfrak{p}+m_\mathfrak{p})(2-1/n)}} \right) \left(1 + \frac{N\mathfrak{p}^{12b_\mathfrak{p}} - c_0^\mathfrak{p}}{N\mathfrak{p}^{6b_\mathfrak{p}(2-1/n)}} \right)^{-1},$$

where $b_\mathfrak{p}$ is defined in Proposition 2 and $1 \leqslant b_\mathfrak{p} \leqslant 1 + 5v_\mathfrak{p}(2) + 2v_\mathfrak{p}(3)$.

Proof. Let S be a set of primes not dividing $\mathfrak{m}$. Define $F(S, \mathfrak{m}; t)$ to be the number of pairs (A, B) with $H([A, B, 1]) \leqslant t$ such that

$$\left(\bar{A}, \bar{B}\right) \text{ for all } C_{m_\mathfrak{p}}^\mathfrak{p} \forall \mathfrak{p}|\mathfrak{m}$$

and

$$\left(\bar{A}, \bar{B}\right) \text{ for all } C_{m_\mathfrak{p}}^\mathfrak{p} \forall \mathfrak{p} \in S.$$

Note that $m_\mathfrak{p} = 0$ for $\mathfrak{p} \in S$. By the inclusion–exclusion principle we have

$$G(\mathfrak{m}, t) = \sum_{i=0}^{\infty} (-1)^i \sum_{\#S=i} F(S, \mathfrak{m}; t).$$

This sum is actually finite because for i large enough, S will contain a prime $\mathfrak{p}$ not dividing 2 or 3 with $N\mathfrak{p} > t^{1/6}$. Since for $\left(\bar{A}, \bar{B}\right) \in F(S, \mathfrak{m}; t)$ we have $\left(\bar{A}, \bar{B}\right) \notin C_0^\mathfrak{p}$ Eq. (3) will not be minimal at $\mathfrak{p}$ which means that $v_\mathfrak{p}(A) \geqslant 4$ and $v_\mathfrak{p}(B) \geqslant 6$ as shown in the proof of Proposition 4. Then we will have $H([A, B, 1]) \geqslant \max\{N(A), N(B)\} \geqslant N\mathfrak{p}^6 > t$ implying $F(S, \mathfrak{m}; t) = 0$. Now we apply Proposition 7 with $\mathfrak{a}_1 = \mathfrak{a}_2 = \mathfrak{a}$ where

$$\mathfrak{a} = \prod_{\mathfrak{p}|\mathfrak{m} \text{ or } \mathfrak{p}\in S} \mathfrak{p}^{6(b_\mathfrak{p}+m_\mathfrak{p})}.$$

Since we have

$$a(\mathfrak{m}, S) = \prod_{\mathfrak{p}|\mathfrak{m}} c_{m_\mathfrak{p}}^{\mathfrak{p}} \prod_{\mathfrak{p}\in S} \left(N\mathfrak{p}^{12b_\mathfrak{p}} - c_0^{\mathfrak{p}} \right)$$

equivalence classes we get

$$F(S, \mathfrak{m}; t) = a(\mathfrak{m}, S) \left(\frac{C_K \operatorname{Vol} R(t)}{N\mathfrak{a}^2} + \mathrm{O}\left(\frac{\operatorname{Vol} \partial R(t)}{N\mathfrak{a}^{2-1/n}} \right) \right).$$

For the main term in $G(\mathfrak{m}, t)$ we need to calculate

$$\sum_{i=0}^{\infty} (-1)^i \sum_{\#S=i} \frac{a(\mathfrak{m}, S)}{N\mathfrak{a}^2}.$$

Since S and $\mathfrak{m}$ are relatively prime the sum above is given by

$$\prod_{\mathfrak{p}|\mathfrak{m}} \frac{c_{m_\mathfrak{p}}^{\mathfrak{p}}}{N\mathfrak{p}^{12(b_\mathfrak{p}+m_\mathfrak{p})}} \prod_{\mathfrak{p}\nmid\mathfrak{m}} \left(1 - \frac{N\mathfrak{p}^{12b_\mathfrak{p}} - c_0^{\mathfrak{p}}}{N\mathfrak{p}^{12b_\mathfrak{p}}} \right)$$

which can also be written as

$$\prod_{\mathfrak{p}|\mathfrak{m}} \frac{c_{m_\mathfrak{p}}^{\mathfrak{p}}}{c_0^{\mathfrak{p}} N\mathfrak{p}^{12m_\mathfrak{p}}} \prod_{\mathfrak{p}} \left(\frac{c_0^{\mathfrak{p}}}{N\mathfrak{p}^{12b_\mathfrak{p}}} \right).$$

The infinite product on the right converges since from Remark 5 for all but finitely many $\mathfrak{p}$ we have $c_0^{\mathfrak{p}} = N\mathfrak{p}^{12}\left(1 - N\mathfrak{p}^{-10}\right)$ and $b_\mathfrak{p} = 1$. It is given by

$$\alpha(K) = \zeta_K(10)^{-1} \prod_{b_\mathfrak{p}>1} \frac{c_0^{\mathfrak{p}}}{\left(1 - N\mathfrak{p}^{-10}\right) N\mathfrak{p}^{12b_\mathfrak{p}}}. \tag{8}$$

For the error term we need the sum

$$\sum_{i=0}^{\infty} \sum_{\#S=i} \frac{a(\mathfrak{m}, S)}{N\mathfrak{a}^{2-1/n}}$$

which is given by

$$\prod_{\mathfrak{p}|\mathfrak{m}} \frac{c_{m_\mathfrak{p}}^{\mathfrak{p}}}{N\mathfrak{p}^{6(b_\mathfrak{p}+m_\mathfrak{p})(2-1/n)}} \left(1 + \frac{N\mathfrak{p}^{12b_\mathfrak{p}} - c_0^{\mathfrak{p}}}{N\mathfrak{p}^{6b_\mathfrak{p}(2-1/n)}} \right)^{-1} \prod_{\mathfrak{p}} \left(1 + \frac{N\mathfrak{p}^{12b_\mathfrak{p}} - c_0^{\mathfrak{p}}}{N\mathfrak{p}^{6b_\mathfrak{p}(2-1/n)}} \right).$$

To show the infinite product converges we reason as above and look at all primes with $b_{\mathfrak{p}} = 1$. We get that

$$\prod_{b_{\mathfrak{p}}=1} \left(1 + \frac{1}{N\mathfrak{p}^{6(2-1/n)-2}}\right)$$

converges since $6(2-1/n)-2 > 1$. Since it is a constant depending only on the field K we omit it in writing the error term and we have the result. □

For $A, B \in K$ we define an ideal $\mathfrak{a}(A,B) = \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}(A,B)}$ where $f_{\mathfrak{p}}(A,B)$ is the function in Proposition 2. Note that $f_{\mathfrak{p}}(A,B) = 0$ for all but finitely many $\mathfrak{p}$. By definition its class is the inverse of the Weierstrass class of the curve given by Eq. (3). With this new definition we can rewrite $G(\mathfrak{m},t)$ from Proposition 9 as

$$G(\mathfrak{m},t) = \#\{A, B : \mathfrak{a}(A,B) = \mathfrak{m}, H([A,B,1]) \leqslant t\}.$$

Proposition 10. *Let K be a number field with class number h_K and let $\mathfrak{C}$ be an ideal class in the class group of K. Let $C(\mathfrak{C},t)$ be the number of integers $A, B \in K$ with $H([A,B,1]) \leqslant t$ and $\mathfrak{a}(A,B)$ in $\mathfrak{C}$. Then,*

$$C(\mathfrak{C},t) = \frac{C_K \operatorname{Vol} R(t)}{h_K \zeta_K(10)} \sum_{\mathfrak{D}} \zeta_K(\mathfrak{D},10) f_K\left(\mathfrak{C}^{-1}\mathfrak{D}\right) + \mathrm{O}\left(\operatorname{Vol} \partial R(t)\right), \tag{9}$$

where $f_K(\mathfrak{D})$ is a real number defined below for any ideal class $\mathfrak{D}$ which can be calculated using information on the class group and finitely many primes of K.

Proof. Let $G(\mathfrak{m},t)$, $g(\mathfrak{m})$, and $f(\mathfrak{m})$ be defined as in Proposition 9. We want to calculate

$$C(\mathfrak{C},t) = \sum_{\mathfrak{m}\in\mathfrak{C}} G(\mathfrak{m},t). \tag{10}$$

For the main term we need

$$\sum_{\mathfrak{m}\in\mathfrak{C}} f(\mathfrak{m})$$

which can be rewritten using orthogonality of character sums as

$$\frac{1}{h_K} \sum_{\chi\in\hat{H}_K} \sum_{\mathfrak{m}} \chi\left(\mathfrak{m}\mathfrak{C}^{-1}\right) f(\mathfrak{m}),$$

where the sum is over all characters on the ideal class group of K. In order to calculate

$$\sum_{\mathfrak{m}} \chi(\mathfrak{m}) f(\mathfrak{m}) = \prod_{\mathfrak{p}} \left(\sum_{k=0}^{\infty} \frac{\chi(\mathfrak{p}^k) c_k^{\mathfrak{p}}}{N\mathfrak{p}^{12k} c_0^{\mathfrak{p}}} \right),$$

we separate the finitely many primes with $b_{\mathfrak{p}} > 1$ and sum using Proposition 4 and Remark 5 and get

$$L(\chi, 10) \prod_{b_{\mathfrak{p}}>1} \frac{1}{c_0^{\mathfrak{p}}} \left(\left(1 - \frac{\chi(\mathfrak{p})}{N\mathfrak{p}^{10}}\right) \sum_{k=0}^{b_{\mathfrak{p}}-2} \frac{\chi(\mathfrak{p}^k) c_k^{\mathfrak{p}}}{N\mathfrak{p}^{12k}} + \frac{c_{b_{\mathfrak{p}}-1}^{\mathfrak{p}} \chi(\mathfrak{p}^{b_{\mathfrak{p}}-1})}{N\mathfrak{p}^{12(b_{\mathfrak{p}}-1)}} \right). \tag{11}$$

Substituting this into Eq. (10) and using Eq. (8) we have

$$\frac{C_K \operatorname{Vol} R(t)}{h_K \zeta_K(10)} \sum_{\chi} \chi\left(\mathfrak{C}^{-1}\right) L(\chi, 10) e_K(\chi),$$

where

$$\begin{aligned} e_K(\chi) = & \prod_{b_{\mathfrak{p}}>1} \frac{\left(1 - N\mathfrak{p}^{-10}\right)^{-1}}{N\mathfrak{p}^{12b_{\mathfrak{p}}}} \\ & \times \left(\left(1 - \frac{\chi(\mathfrak{p})}{N\mathfrak{p}^{10}}\right) \sum_{k=0}^{b_{\mathfrak{p}}-2} \frac{\chi(\mathfrak{p}^k) c_k^{\mathfrak{p}}}{N\mathfrak{p}^{12k}} + \frac{c_{b_{\mathfrak{p}}-1}^{\mathfrak{p}} \chi(\mathfrak{p}^{b_{\mathfrak{p}}-1})}{N\mathfrak{p}^{12(b_{\mathfrak{p}}-1)}} \right) \end{aligned} \tag{12}$$

for the main term. We can write $L(\chi, 10)$ as

$$L(\chi, 10) = \sum_{\mathfrak{D}} \chi(\mathfrak{D}) \zeta_K(\mathfrak{D}, 10),$$

where the sum is over all ideal classes $\mathfrak{D}$ and $\zeta_K(\mathfrak{D}, s)$ is the partial zeta function. Summing over all the characters we have the desired result with $f_K(\mathfrak{D})$ being defined by

$$f_K(\mathfrak{D}) = \sum_{\chi} \chi(\mathfrak{D}) e_K(\chi) \tag{13}$$

for any ideal class $\mathfrak{D}$. Since the conjugate of a character is its inverse, we immediately see that $f_K(\mathfrak{D})$ is a real number for any ideal class $\mathfrak{D}$. For the error term we need to

calculate

$$\sum_{\mathfrak{m}} g(\mathfrak{m}) = \prod_{\mathfrak{p}} \left(1 + \sum_{k=1}^{\infty} g\left(\mathfrak{p}^k\right)\right).$$

Since we are only interested in convergence it suffices to take the product over all but finitely many primes, so we can discard the primes with $b_{\mathfrak{p}} > 1$. Then the product becomes

$$\prod_{b_{\mathfrak{p}}=1} \left(1 + \left(1 + \frac{N\mathfrak{p}^{12} - c_0^{\mathfrak{p}}}{N\mathfrak{p}^{6(2-1/n)}}\right)^{-1} \sum_{k=1}^{\infty} \frac{c_0^{\mathfrak{p}} N\mathfrak{p}^{2k}}{N\mathfrak{p}^{6(k+1)(2-1/n)}}\right)$$

which after summing up the geometric series is given by

$$\prod_{b_{\mathfrak{p}}=1} \left(1 + \left(1 + \frac{1}{N\mathfrak{p}^{12(2-1/n)-4}}\right)^{-1} \frac{\left(1 - N\mathfrak{p}^{-10}\right)}{N\mathfrak{p}^{12(2-1/n)-14}}\right).$$

This product converges since $12(2 - 1/n) - 14 \geqslant 4$. So the error term has a constant depending only on the number field K. Substituting (11) into (10) we have the result. □

Theorem 11. *Let K be a number field and let $\mathfrak{C}$ be an ideal class in the ideal class group of K. Let $N(\mathfrak{C}, t)$ be the number of $A, B \in O_K$ such that $y^2 = x^3 + Ax + B$ defines an elliptic curve with $\mathfrak{a}_\Delta$ in $\mathfrak{C}$ and $H([A, B, 1]) \leqslant t$ and let $D(t) = \sum_{\mathfrak{C}} N(\mathfrak{C}, t)$. Then the asymptotic density of elliptic curves having Weierstrass class equal to $\mathfrak{C}$ is given by*

$$\lim_{t\to\infty} \frac{N(\mathfrak{C}, t)}{D(t)} = \frac{1}{h_K \zeta_K(10)} \sum_{\mathfrak{D}} \zeta_K(\mathfrak{D}, 10) f_K(\mathfrak{C}\mathfrak{D}), \tag{14}$$

where $\zeta_K(s)$ is the Dedekind zeta function, $\zeta_K(\mathfrak{D}, s)$ is the partial zeta function for an ideal class $\mathfrak{D}$ of K, the sum is over all ideal classes,

$$f_K(\mathfrak{D}) = \sum_{\chi} \chi(\mathfrak{D}) e_K(\chi)$$

with $e_K(\chi)$ defined by Eq. (12) *above. Moreover, this density is a positive number for any class $\mathfrak{C}$.*

Proof. Let $d(t) = \#\left\{A, B \in O_K : 4A^3 + 27B^2 = 0, H([A, B, 1]) \leqslant t\right\}$. Then it is clear that

$$N\left(\mathfrak{C}, t\right) = C\left(\mathfrak{C}^{-1}, t\right) + \mathrm{O}\left(d(t)\right),$$

where $C\left(\mathfrak{C}, t\right)$ is the counting function defined in Proposition 10 and

$$D(t) = F\left(O_K, O_K; t\right) + \mathrm{O}\left(d(t)\right).$$

Since

$$\begin{aligned} d(t) &= \mathrm{O}\left(\#\left\{\alpha \in O_K : H\left(\left[-3\alpha^2, 2\alpha^3, 1\right]\right) \leqslant t\right\}\right) \\ &= \mathrm{O}\left(\#\left\{\alpha \in O_K : H\left(\left[\alpha^3, 1\right]\right) \leqslant t\right\}\right) \\ &= \mathrm{O}\left(t^{1/3}(\log t)^r\right) \end{aligned}$$

using Proposition 7 and Remark 8 we have

$$D(t) = C_K t^2 (\log t)^r + \mathrm{O}\left(t^2 (\log t)^{r-1}\right)$$

and from Proposition 10 together with Remark 8 again we have

$$N\left(\mathfrak{C}, t\right) = \frac{C_K t^2 (\log t)^r}{h_K \zeta_K(10)} \sum_{\mathfrak{D}} \zeta_K\left(\mathfrak{D}, 10\right) f_K\left(\mathfrak{C}\mathfrak{D}\right) + \mathrm{O}\left(t^2 (\log t)^{r-1}\right).$$

Taking the limit as t goes to infinity of the quotient we get the result. In order to prove that it is indeed a positive number, we need to remember how we got this formula. The result given by Eq. (14) is actually

$$\alpha(K) \sum_{\mathfrak{m} \in \mathfrak{C}^{-1}} f(\mathfrak{m}).$$

Here $\alpha(K)$ is clearly positive. As for the sum, let $\mathfrak{p}$ be any prime not dividing 6 in the class $\mathfrak{C}^{-1}$. Then a lower bound for $\sum_{\mathfrak{m} \in \mathfrak{C}^{-1}} f(\mathfrak{m})$ is given by $f(\mathfrak{p}) = N\mathfrak{p}^{-10}$ which proves that the result must be positive for any ideal class. □

Although the result given by Eq. (14) is a complicated expression, in some cases it can be simplified. The next proposition limits the primes we must consider for $e_K(\chi)$ appearing in the formula for the constants $f_K\left(\mathfrak{D}\right)$.

Proposition 12. *If $b_{\mathfrak{p}} > 1$ for some prime $\mathfrak{p}$ then either $\mathfrak{p}|2$ or $\mathfrak{p}|3$ and $v_{\mathfrak{p}}(3) > 1$. Moreover, if $\chi(\mathfrak{p}) = 1$ then we can exclude the $\mathfrak{p}$ factor from the product for the quantity $e_K(\chi)$ defined in Proposition* 10.

Proof. As we mentioned in Remark 5, $b_{\mathfrak{p}} > 1$ implies $\mathfrak{p}|2$ or $\mathfrak{p}|3$. If $\mathfrak{p}|3$ and $v_{\mathfrak{p}}(3) = 1$ an easy application of Tate's algorithm [7] shows that the Eq. (3) is minimal if $v_{\mathfrak{p}}(A) < 4$ or $v_{\mathfrak{p}}(B) < 6$ which implies that $b_{\mathfrak{p}} = 1$. If we undo the sum of the geometric series appearing in $e_K(\chi)$ we can see that each term of the product is given by

$$\frac{\left(1 - N\mathfrak{p}^{-10}\right)}{\left(1 - \frac{\chi(\mathfrak{p})}{N\mathfrak{p}^{10}}\right)} \sum_{k=0}^{\infty} \frac{\chi\left(\mathfrak{p}^k\right) c_k^{\mathfrak{p}}}{N\mathfrak{p}^{12(b_{\mathfrak{p}}+k)}}.$$

If $\chi(\mathfrak{p}) = 1$ then it reduces to

$$\sum_{k=0}^{\infty} \frac{c_k^{\mathfrak{p}}}{N\mathfrak{p}^{12(b_{\mathfrak{p}}+k)}} = 1 \tag{15}$$

since $\left(\bar{A}, \bar{B}\right) \in C_k^{\mathfrak{p}}$ for some k. □

Corollary 13. *Let K be a number field such that all primes above* 2 *are principal and such that all ramified primes above* 3 *are principal. Then the density of elliptic curves over K having a global minimal equation is given by*

$$\frac{\zeta_K\left(\mathfrak{C}_0, 10\right)}{\zeta_K(10)},$$

where $\mathfrak{C}_0$ is the class of principal ideals.

Proof. In this case $e_K(\chi)$ is the empty product for any χ and the only non-zero $f_K\left(\mathfrak{D}\right)$ is with $\mathfrak{D} = \mathfrak{C}_0$ which is $f_K\left(\mathfrak{C}_0\right) = h_K$. □

4. Examples

Let $K = \mathbb{Q}\left(\sqrt{65}\right)$. The field K has class number 2, the prime 3 is unramified, and the prime 2 splits into two non-principal primes. By Proposition 12 we only need to consider the primes $\mathfrak{p}$ above 2 to calculate $e_K(\chi)$. In the following lemma we determine the minimality conditions of Eq. (3) at the primes $\mathfrak{p}|2$.

Lemma 14. *The equation $y^2 = x^3 + Ax + B$ where $A, B \in O_{\mathfrak{p}}$ is minimal at $\mathfrak{p}$ unless $v_{\mathfrak{p}}(A) \geqslant 4$ and $v_{\mathfrak{p}}(B) \geqslant 6$ or $v_{\mathfrak{p}}(A) \geqslant 4$ and $v_{\mathfrak{p}}(B - 16) \geqslant 6$. When $v_{\mathfrak{p}}(A) \geqslant 4$ and*

$v_{\mathfrak{p}}(B-16) \geqslant 6$, *there exists a change of variables with* $v_{\mathfrak{p}}(u) = 1$ *resulting in a minimal equation.*

Proof. If $v_{\mathfrak{p}}(A) \geqslant 4$ and $v_{\mathfrak{p}}(B) \geqslant 6$ the equation is obviously not minimal. So assume $v_{\mathfrak{p}}(A) < 4$ or $v_{\mathfrak{p}}(B) < 6$. Since 2 is unramified, we can take 2 as a uniformizer. In the following cases, $v_{\mathfrak{p}}(\Delta) < 12$ so the equation must be minimal: $v_{\mathfrak{p}}(B) = 0$, $v_{\mathfrak{p}}(B) = 2$, $v_{\mathfrak{p}}(B) = 3$, $v_{\mathfrak{p}}(B) = 1$ and $v_{\mathfrak{p}}(A) \geqslant 1$, $v_{\mathfrak{p}}(B) \geqslant 4$ and $v_{\mathfrak{p}}(A) \leqslant 1$. In the remaining cases easy applications of Tate's algorithm [7] show the equation is minimal unless $v_{\mathfrak{p}}(A) \geqslant 4$ and $v_{\mathfrak{p}}(B) = 4$. When $v_{\mathfrak{p}}(A) \geqslant 4$ and $v_{\mathfrak{p}}(B) = 4$ we can make a change of variables by shifting y to get

$$y^2 + 8y = x^3 + Ax + B - 16.$$

Since the residue field is $\mathbb{F}_2$ and $v_{\mathfrak{p}}(B) = 4$, we get that $v_{\mathfrak{p}}(B-16) \geqslant 5$. Once again Tate's algorithm shows that the equation is minimal unless $v_{\mathfrak{p}}(B-16) \geqslant 6$. But since $v_{\mathfrak{p}}(B) = 4$ the valuation of the discriminant is 12. Since the change of variables decreases the valuation of the discriminant by $12v_{\mathfrak{p}}(u)$ we must have $v_{\mathfrak{p}}(u) = 1$. □

Now we need to find $b_{\mathfrak{p}}$. Note that from Eq. (15) once we know $c_0^{\mathfrak{p}}, \ldots, c_{b_{\mathfrak{p}}-2}^{\mathfrak{p}}$ then $c_{b_{\mathfrak{p}}-1}^{\mathfrak{p}}$ can be calculated. Therefore, $b_{\mathfrak{p}} = 1$ if and only if $c_0^{\mathfrak{p}} = N\mathfrak{p}^{12}\left(1 - N\mathfrak{p}^{-10}\right)$. So the above lemma shows that $b_{\mathfrak{p}} \geqslant 2$. But the lemma also completely determines those A, B which give a minimal Weierstrass equation. Therefore $b_{\mathfrak{p}} = 2$ and it suffices to calculate $c_0^{\mathfrak{p}}$. A simple counting argument with the characterization of the lemma together with the fact that $N\mathfrak{p} = 2$ gives

$$c_0^{\mathfrak{p}} = N\mathfrak{p}^{24} - \#\left(\frac{\mathfrak{p}^4}{\mathfrak{p}^{12}} \times \frac{\mathfrak{p}^6}{\mathfrak{p}^{12}}\right) - \#\left(\frac{\mathfrak{p}^4}{\mathfrak{p}^{12}} \times \frac{\mathfrak{p}^2}{\mathfrak{p}^8}\right) = 2^{24} - 2^{15}.$$

From this using Eq. (15) we can also calculate $c_1^{\mathfrak{p}}$. Now we are ready to calculate $f_K(\mathfrak{C})$ for the two ideal classes. Let $\mathfrak{C}_0$ be the class of principal ideals and $\mathfrak{C}_1$ be the non-trivial class. We have

$$f_K(\mathfrak{C}_0) = \frac{46026876023776399 45}{4602683217219158016}, \qquad f_K(\mathfrak{C}_1) = \frac{4602678832060676087}{4602683217219158016}.$$

Now the density of elliptic curves over K having a global minimal Weierstrass equation is given by

$$\frac{1}{h_K \zeta_K(10)}\left(\zeta_K(\mathfrak{C}_0, 10) f_K(\mathfrak{C}_0)\right) + \zeta_K(\mathfrak{C}_1, 10)\left(f_K(\mathfrak{C}_1)\right).$$

For real quadratic fields, the Dedekind zeta function can be evaluated using Dirichlet L-series and the partial zeta functions can be evaluated using a method due to Shintani

[4]. Hence, in this particular instance we can give an exact answer. The density of elliptic curves over $\mathbb{Q}\left(\sqrt{65}\right)$ having a global minimal Weierstrass equation is

$$\frac{2756803340602040492415758477747 09}{5513601448658505641719593172992 00} \approx \frac{1}{2} + 10^{-6.324}.$$

This brings up the question of whether in general there is an approximately even distribution among ideal classes. The answer is no. For example the quadratic number field $\mathbb{Q}\left(\sqrt{85}\right)$ has class number 2, the prime 3 is unramified and the prime 2 is inert. It satisfies the hypotheses of Corollary 13 and hence the ratio can be calculated by the simpler formula given in the corollary. In this case we find that the ratio of elliptic curves defined over $\mathbb{Q}\left(\sqrt{85}\right)$ which have a global minimal Weierstrass equation is

$$\frac{67271573838501913}{67273859703467650} \simeq 1 - 10^{-4.469}.$$

In fact, for any number field K of degree n satisfying the hypotheses of Corollary 13 the ratio of elliptic curves defined over K which have a global minimal Weierstrass equation is greater or equal to 0.999^{-n} because

$$\frac{\zeta_K\left(\mathfrak{C}_0, 10\right)}{\zeta_K\,(10)} \geqslant \frac{1}{\zeta_K\,(10)} \geqslant \zeta\,(10)^{-n} \geqslant 0.999^{-n}.$$

Acknowledgments

This paper includes some of the results from the author's Ph.D. Thesis (Brown University, May 2002). The author would especially like to thank her advisor, Joseph Silverman, for his encouragement and guidance. The author also thanks Siman Wong for helpful conversations on the contents of this paper. Finally, the author thanks the referee for his careful reading of the manuscript and for many useful comments.

References

[1] J.W.S. Cassels, An Introduction to the Geometry of Numbers, Springer, Berlin, 1971.
[2] A. Fröhlich, The discriminants of relative extensions and the existence of integral bases, Mathematika 7 (1960) 15–22.
[3] S. Lang, Algebraic Number Theory, Springer, Berlin, 1994.
[4] T. Shintani, On evaluation of zeta functions of totally real algebraic number fields at non-positive integers, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 23 (1976) 393–417.
[5] J.H. Silverman, Weierstrass equations and the minimal discriminant of an elliptic curve, Mathematika 31 (1984) 245–251.
[6] J.H. Silverman, The Arithmetic of Elliptic Curves, Springer, Berlin, 1986.
[7] J. Tate, Algorithm for Determining the Type of a Singular Fiber in an Elliptic Pencil, Lecture Notes in Mathematics, vol. 476, Springer, Berlin, 1975, pp. 33–52.